

EPMACINST 5510.1J
Code 40D
11 December 2001

EPMAC INSTRUCTION 5510.1J

Subj: CLASSIFIED MATERIAL CONTROL PROGRAM

Ref: (a) SECNAVINST 5510.36
(b) OPNAVINST 5510.30A

Encl: (1) Control and Handling of Classified Material
(2) Classified Information Security Check List

1. Purpose. To provide policy and procedures within the Enlisted Placement Management Center (EPMAC) on matters relating to Classified Material Control Program per references (a) and (b), and maintain control of classified material as provided in enclosures (1) and (2). This instruction has been changed in its entirety and should be completely reviewed.

2. Cancellation. EPMACINST 5510.1H

3. Action

a. The Commanding Officer (CO) is ultimately responsible for the Classified Material Control Program at EPMAC.

b. The Command Security Manager is the principal advisor to the CO on information security, and will perform duties prescribed in references (a) and (b).

c. The Classified Material Control Officer reports to the Command Security Manager and also coordinates with the Physical and Personnel Security Officers in the performance of this duty.

G. SHEEHAN

Distribution:
EPMAC Intranet

CONTROL AND HANDLING OF CLASSIFIED MATERIAL

1. Objective. To preclude the loss or unauthorized disclosure of classified material within EPMAC and to ensure EPMAC classified material procedures conform to the provisions of references (a) and (b).

2. Policy. Access to classified material will be granted only to those personnel with proper security clearances, who have been granted access.

3. Accountability

a. Top Secret. Top Secret material or messages are not held by EPMAC. Top Secret messages are reviewed by an individual required to have a Top Secret clearance. Once the individual reviews the messages, they are destroyed by NTCC.

b. Secret and Confidential. Mail containing secret and confidential documents must meet the accountability requirements of reference (a).

4. Mode of Transmission of Classified Material

a. Telephones. Classified information may be transmitted via secure telephone units (STU III).

b. Fax. Facsimile equipment or similar devices using unsecure telephone lines will not be used to transmit classified information.

c. Computer. Classified messages shall not be processed on computers not designated to process classified material. Additionally, classified messages shall not be processed electronically as attachments to emails.

5. Destruction of Classified Material. The equipment for shredding classified material is located in EPMAC's mail room.

6. Classified Messages. The Classified Control Clerk receives classified messages from the Information Systems Technology Department. The messages are put in routing for control, reviewed by appropriate codes, and once any necessary action is taken, the messages are destroyed.

EPMACINST 5510.1J
11 December 2001

7. Authorized Recipients of Classified Material. Director, Administrative Services Office is responsible for preparing and distributing the Security Access List.

8. Security Containers. All classified material will be stored in GSA approved safes. The SF 702, Security Container Check Sheet, will be filled out when opening and closing safes that contain classified material.

9. Responsibilities of Safe Custodians. Information for safe control is contained in references (a) and (b).

CLASSIFIED INFORMATION SECURITY CHECK LIST

1. Each individual must be sure his or her working area is secure at the end of the working day.
 - a. Look on top of, under, behind, and in desks.
 - b. Make sure that working trays and baskets are empty.
 - c. Properly store or shred notes, carbon paper, rough drafts, or similar working papers.
 - d. Place classified documents, correspondence, or related classified material in proper security containers.
 - e. The disks and printer ribbons are removed from word processors and Personal Computers (PC's) and the electrical power is turned off.
 - f. Securely close each drawer or door of the security container and lock the container by rotating the dial at least four complete turns in the same direction.
 - g. Check the locking drawer to make sure the container is secured.
 - h. Survey the general area to be sure no classified material is unsecured. This includes looking on top of and in between security containers, general storage cabinets, working tables, and checking trash cans.
 - i. Double check security containers to ensure they are closed and locked by rotating the combination dial four times in the same direction and trying to open each drawer of the security containers.
 - j. The reproduction machine is cleared by running it once and checking the reproduction paper for impressions. Machines will be turned off at the end of the working day.
 - k. The fax is cleared.
 - l. Security container tops are cleared.
 - m. Individual office spaces are cleared.

EPMACINST 5510.1J
11 December 2001

n. Typewriter ribbons are removed from those machines using carbon ribbons on which classified information has been typed.

o. Any electrical appliances are disconnected.

p. The general area is surveyed.

q. If anyone is still working in the area, with a security container open, he or she is listed as an exception, beside the item on the checklist which has not been secured. That person will then be responsible for securing the item, double checking, and initialing the checklist, showing the time of securing.